UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/059,217	01/31/2002	Mikio Hashimoto	218943US2RD	6024

22850 7590 02/14/2006

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 02/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/059,217	HASHIMOTO ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-9 and 11-13* is/are pending in the application.

4a) Of the above claim(s) *11 and 12* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-9 and 13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. No claim for priority has been made in this application.

The effective filing date for the subject matter defined in the pending claims in this application is 1/31/2002.

Original application contained claims 1 – 11. Claims 1 and 10 have been canceled; claims 2, 4, 5, 9 and 11 have been amended; and new claims 12 and 13 have been added in an amendment filed on 12/28/2005. Claims 11 – 12 are withdrawn from further consideration by the Examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention. The amendment filed have been entered and made of record. Presently, pending claims are elected Group I: Claims 2 – 9 and 13.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 1/31/2002 has been entered.

During a telephone conversation with Attorney Eckhard H. Kuesters on January 30, 2006, a provisional election was made without traverse to prosecute the invention of Group I: Claims 2 – 9 and 13. Affirmation of this election must be made by Applicant in replying to this Office action. Claims 11 – 12 are withdrawn from further consideration by the Examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Election / Restrictions

This application contains claims directed to the following patentably distinct claimed inventions. Restriction to one of the following invention is required under 35 U.S.C 121:

I. (Group 1) Claims 2 – 9 and 13 drawn to a system for providing a secret key specific to the microprocessor that cannot be read to an external device for computer instruction / data encryption and using an asynchronous notification upon a completion of key registration to the processor, classified in class 713, subclass 191.

II. (Group 2) Claims 11 drawn to a system for providing a secret key specific to the microprocessor that cannot be read to an external device by using the secret key to obtain the instruction key and feedback key for instruction / data encryption, classified in class 713, subclass 190.

III. (Group 3) Claim 12 drawn to a system for providing a secret key specific to the microprocessor that cannot be read to an external

device by using a perpetuation flag indicating the permission and protection of a context saving, classified in class 713, subclass 193.

Inventions I – III are related as combination and subcombination disclosed as usable together in a single combination. The subcombination is distinct from the combination and the subcombinations are distinct from each other if they are shown to be separately usable. The following case instants:

Invention I has utility directed to a system for providing a secret key specific to the microprocessor including plaintext instruction s and encrypted instructions and using an asynchronous notification upon a completion of key registration to the processor.

Invention II has separate utility directed to a more specific data processing system protection by using a feedback key in obtaining feedback information by encrypting the instruction key when the feedback information is to be written to the external memory.

Invention III has separate utility directed to a system for providing a secret key specific to the microprocessor that cannot be read to an external device by using a perpetuation flag indicating the permission and protection of a context saving in which the instruction key is encrypted by using a prescribed secret key of the microprocessor and written into the external memory.

Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification and utility restriction for examination purpose as indicated is proper.

Examiner acknowledges that Applicant has elected Group I and as such this Office action only addresses the claimed inventions of Group I: Claims 2 – 9 and 13.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 13 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 13 is indefinite because the claim language "wherein the processor core continues executing the instructions during the key registration" is not clear what "continues executing the instructions" the Applicant is exactly referred to because the instructions should be associated with the antecedent basis of the previous claim limitation "a processor core configured to execute instructions of a program" and the later claim limitation "the instruction key is registered in correspondence to a specific program". Therefore, it is not clear what "continues executing the instructions" is exactly

referred to – e.g. either associated with the same program or another program, which is required to be particularly pointed out and distinctly claimed for this subject matter.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claim 13 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

The claim limitation of claim 13 "wherein the processor core continues executing the instructions during the key registration" is not enabled by the specification because the instructions should be associated with the antecedent basis of the previous claim limitation "a processor core configured to execute instructions of a program" and the later claim limitation "the instruction key is registered in correspondence to a specific program". However, as understood by the examiner, "continue execution of instructions" should be referred to another / different program according to the specification, Page 16 Line 10 – 12. Therefore, the invention of claim limitation is not clearly and concisely defined / specified in a manner which can be carried out by one skilled in the art.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 13 and 2 – 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hartman (Patent Number: 5224166), in view of Alexander (Patent Number: 6188602).

As per claim 13, Hartman teaches a microprocessor internally having a secret key specific to the microprocessor that cannot be read out to an external, the microprocessor comprising:

a processor core configured to execute instructions of a program including plaintext instructions and encrypted instructions, the encrypted instructions being encrypted by using an instruction key specific to the program (Hartman, Column 3 Line 18 – 20 and Column 4 Line 20 – 22: MMK key is equivalent to the instruction key; and

a key management unit configured to carry out a key registration for reading out from an external memory a distribution key that is obtained in advance by encrypting the instruction key by using a public key corresponding to the secret key, decrypting the distribution key by using the secret key to obtain the instruction key, and registering the instruction key in correspondence to a specific program identifier for identifying the

program into a key table (Hartman, Column 4 Line 53 – 57 and Column 5 Line 59 – 64: the master key (i.e. instruction key) is saved into a secure physical region after being decrypted by the private key – this is considered as equivalent to a registration process).

Hartman does not teach using an interrupt to notify asynchronously the completion of the key registration.

Alexander teaches a mechanism to notify a completion of the key registration to the processor core asynchronously by interruption when the key registration is completed, wherein the processor core continues executing the instructions during the key registration by the key management unit and starts to execute the program by using the corresponding instruction key after receiving notification of the implementation of the key registration from the key management unit (Hartman, Column 4 Line 50 – 57, Alexander, Column 1 Line 60 – 65, Column 2 Line 22 – 32 and Column 5 Line 57 – 62: SMI (Interrupt) is used to update the protected information (i.e. medium master key) residing in flash memory via locking / unlocking mode during the system normal computer system operation. Examiner notes (a) the Hartman reference is relied upon providing a mechanism that upon a completion of a key registration to the processor core when the key registration is completed, a clear copy of the media master key is then stored into a secure physical memory region (Hartman: Column 4 Line 50 – 57), and (b) Alexander is relied upon providing a SMI interrupt (System Management Interrupt) to unlock the flash memory to update or change protected information in flash memory (Alexander: Column 5 Line 58 – Column 6 Line 2) and (c) multi-tasking is a

commonly used technique in the field and thereby continue executing another task / program while waiting for the completion of the key registration process of the current task should be an obvious design practice for software engineering).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Alexander's SMI (System Management Interrupt) within the system of Hartman's instruction key registration process because it offers the advantages of allowing the system to update the protected critical information in parallel to the system normal operation and thereby considerably reducing the platform complexity and improving system reliability (Alexander, Column 2 Line 22 – 32 and Column 1 Line 35 – 36).

As per claim 2, Hartman teaches an instruction cache memory configured to store a cache line containing a part of the instructions of the program in correspondence to the specific program identifier (Hartman: Column 3 Line 56 – 58 and Column 4 Line 39 – 40: Examiner notes Hartman teaches the non-encrypted instructions (after decryption) are directly stored in the internal memory cache (Hartman: Column 3 Line 56 – 58) and each of the desired media has the media identifier (Hartman: Column 4 Line 39 – 40: a media identifier is considered as a program ID)), and permit reading of the cache line only when the specific program identifier stored in correspondence to the cache line coincides with a program identifier received along with a program reading request from the processor core; wherein the key management unit is also configured to carry out a flashing of the cache line stored in correspondence to the specific program

identifier on the cache memory when the key management unit rewrites the instruction key corresponding to the specific program identifier in the key table (Hartman, Column 3 Line 56 – 58 and Column 7 Line 32 – 35).

As per claim 3, Hartman further teaches the key management unit carries out the flashing in parallel to the key registration, and notifies the completion of the key registration to the processor core when the key registration and the flashing are both completed (Hartman, Column 4 Line 50 – 57, Alexander, Column 1 Line 60 – 65, Column 2 Line 22 – 32 and Column 5 Line 57 – 62: SMI (Interrupt) is used to update the protected information residing in flash memory via locking / unlocking mode during the system normal computer system operation).

As per claim 4, Hartman further teaches an instruction decryption processing unit configured to decrypt the encrypted instructions of the program read out from the external memory, by using the instruction key registered in correspondence to the specific program identifier by the key management unit, according to a chain information indicating chain relationships among encryption blocks in units of which the encrypted instructions are encrypted (Hartman, Figure 2 Element 56, Column 4 Line 20 – 22 , Column 5 Line 51 – 55 and Column 6 Line 9 – 15: each one of encrypted multiple code segments can be considered as a encryption block in units of which the encrypted instructions are encrypted. Examiner notes Hartman teaches a variety of program segments classified as code segments, data segments and stack segments contain the

media master key that is to be used in decryption or encryption of information in the corresponding memory segments and the relationships among the code segment, data segment and stack segment must be closely-tied to assure the proper operation of the system with respect to normal operations and context saving operations).

As per claim 5, Hartman further teaches the key management unit is also configured to register a data key to be used in encrypting/decrypting data for the program in correspondence to the specific program identifier into the key table (Hartman, Column 4 Line 20 – 22, Column 5 Line 54 and Column 6 Line 5 – 8: the master key associated with data segment can be considered as the data key).

As per claim 6, Hartman further teaches a key index conversion unit configured to convert a set of a program identifier and a key type identifier received from the processor core into a corresponding key value index; and a decryption processing unit configured to decrypt encrypted instructions or data of a program specified by the program identifier received from the processor core and read out from the external memory, by using an instruction key or a data key indexed by the corresponding key value index obtained by the key index conversion unit (Hartman, Column 4 Line 20 – 22, Column 5 Line 51 – 55 and Column 6 Line 5 – 15: the key type can be either instruction key, data key or stack (context-switch) key which is associated with code segment, data segment or stack segment as taught by Hartman).

As per claim 7, Hartman further teaches the key index conversion unit converts more than one sets of a program identifier and a key type identifier into an identical key value index (Hartman, Column 4 Line 20 – 22 & Column 4 Line 33 – 34 and Column 5 Line 51 – 55, Column 6 Line 5 – 15).

As per claim 8, Hartman further teaches a cache memory configured to store a part of instructions or data of programs by using key value indexes obtained by the key index conversion unit as cache tags (Hartman, Column 7 Line 32 – 40, Column 4 Line 20 – 22 & Column 4 Line 33 – 34 and Column 5 Line 51 – 55, Column 6 Line 5 – 15: a data cache associated with an encrypted data segment using a flag to associated with the situation whether the corresponding code segment is encrypted or not).

As per claim 9, Hartman further teaches the key management unit is also configured to register a data key to be used in encrypting/decrypting data for the program in correspondence to the specific program identifier into the key table (Hartman, Column 4 Line 20 – 22, Column 5 Line 54 and Column 6 Line 5 – 8: the master key associated with stack segment can be considered as the context-switch key where stack segment is used during the context switching of the CPU operation due to a context saving).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100